2016

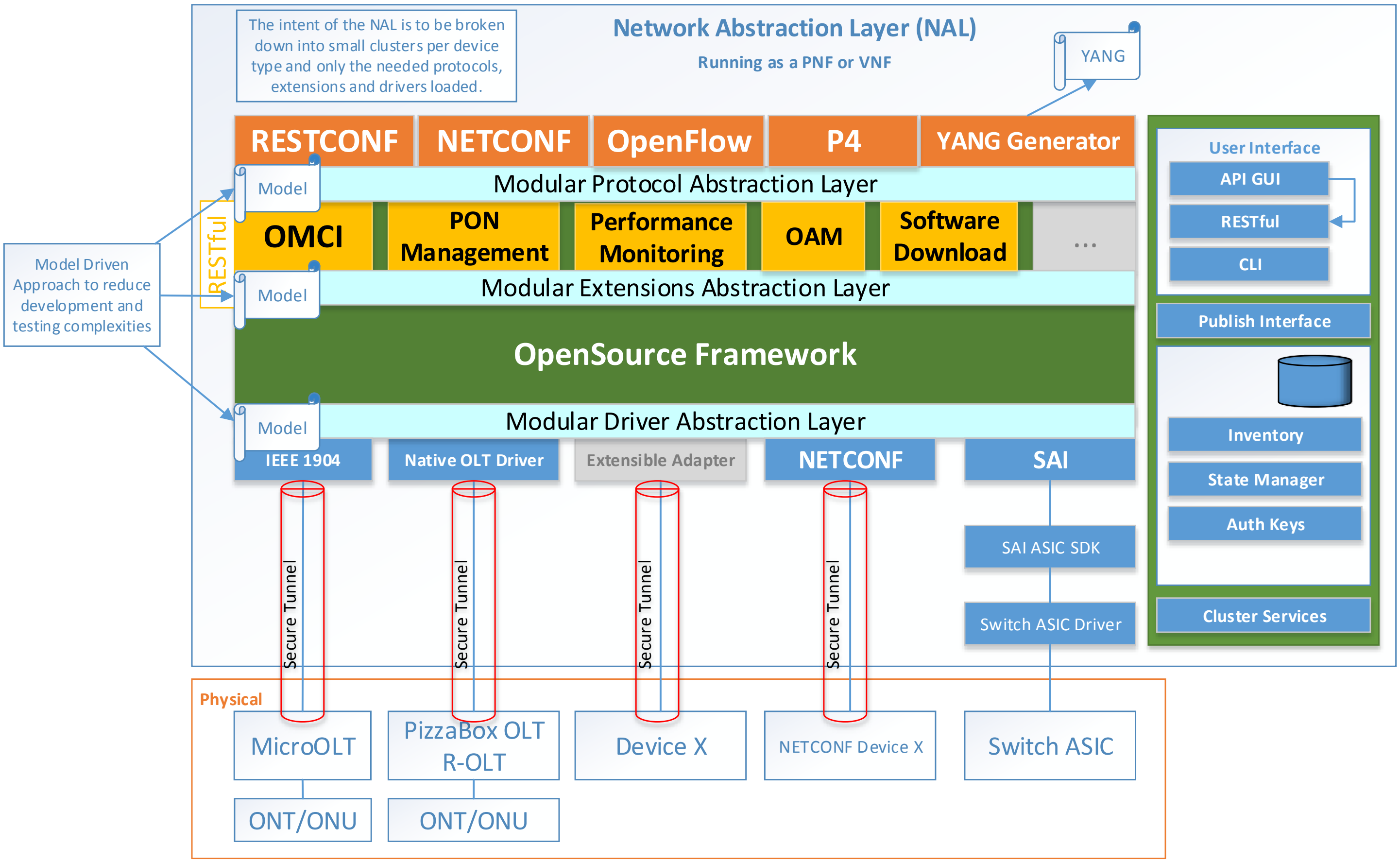
EPIC 1

NETWORK ABSTRACTION LAYER (NAL)

Table of Contents

Introduction

As a service provider, we want to have an OpenSource extensible framework to disaggregate and standardize the protocols and data management from various network hardware implementations. Having a consistent framework for protocols and interface models will allow AT&T to reduce overall infrastructure costs and impacts when introducing new hardware. Initial implementation should support NETCONF for management, OpenFlow for control plane, extensions for PON Management, Performance Management, OAM functions and virtualized OMCI (vOMCI).



Assumptions

- A standard set of functions is identified and documented for this Standard OLT mode
- All components will utilize an OpenSource model (excluding drivers).
- Common requirements are met that are provided in EPIC_COMMON.docx

Acceptance Criteria

- Ability to change the physical hardware w/o changing or manipulating the interfaces of ONOS or the NAL protocols.
- Support the functionality mapping from common framework to device specific drivers
- Device event and performance collection in a uniform way.
- Provide event and performance data to a Kafaka based publishing interface
- Expose management functions required to operate the physical network device
- Operate in as a n+1 active cluster with the ability to shift management of device to peer nodes with little to no disruption in service
- Abstract all OLT device functions in a uniform way and expose through a consistent interface model
- Meet the defined test plan developed. To be delivered 4Q2016

1.0.1 – NAL General Requirements

Requirement ID	Requirement Description 1.0.1 – NAL General Requirements	RFP Requirement ID
1.0.1.1	NAL shall abstract network flow and management protocols in an extensible way to not impact the core framework.	
1.0.1.2	NAL shall abstract the driver abstraction through the use of YANG models	
1.0.1.3	NAL shall provide an extensibility interface for modular code	
1.0.1.4	NAL shall abstract a driver interface to interact with various hardware implementations utilizing vendor drivers or abstraction layers	
1.0.1.5	NAL shall provide a CLI interface	
1.0.1.6	Shall provide capabilities to provide information through a Kafka Publishing Interface, SFTP and NETCONF	HA 1230
1.0.1.7	Provide UML and documentation for YANG Models.	HA 730
1.0.1.8	Ability to generate standard YANG models based on device capabilities.	HA 720
1.0.1.9	Support Bulk Stats, Accounting and Inventory. Information shall be exposed through a NETCONF interface	HA 1140
1.0.1.10	Shall support OpenFlow [v1.0, v1.3, 1.5 and v2.x in future].	E 1250
1.0.1.11	Shall support NETCONF 1.0 and 1.1 over SSH	
1.0.1.12	Shall support YANG 1.0 and 1.1	
1.0.1.13	Shall support RESTCONF	
1.0.1.14	Will support multiple operating models; bare metal, on OLT NE, Docker Container or KVM Virtual Machine.	HA 130, A 250
1.0.1.15	Hardware abstraction layer, extensions, protocols and any driver connectivity must be provided as an OpenSource contribution to ON.Lab with an Apache 2.0 License	HA 141
1.0.1.16	Shall be modular and extensible to support future protocols, drivers and extensions.	HA 160
1.0.1.17	System shall support time synchronization methods over NTP, PTP, BITS or IEEE 1588 Timing	HA 180
1.0.1.18	Each instance of the Hardware Abstraction shall support the control and management plane various network devices	HA 194
1.0.1.19	All components of the Hardware abstraction shall be contributed to ON.Lab as an OpenSource Project (Excluding the driver code itself and Protocol software	HA 196

Requirement ID	Requirement Description 1.0.1 – NAL General Requirements	RFP Requirement ID
	that exist as an existing OpenSource project)	
1.0.1.20	All ONT and OLT capabilities will be configurable and monitored through a NETCONF interface.	HA 200
1.0.1.21	All commands on the Network device should be exposed as Create-Read-Update-Delete (CRUD) functions.	HA 210
1.0.1.22	Provide topology information for the OLT and ONT.	HA 230, HA 320
1.0.1.24	The NE, upon receiving a configuration command, shall be capable of deleting provisioning data. If the mechanics of deleting a parameter is service affecting, then this function shall be executed only after the involved Network Device resource is placed in the Out-Of-Service state.	HA 260
1.0.1.25	All Control Communication will be abstracted by the vOLT to an OpenFlow 1.3 or greater.	HA 300
1.0.1.26	All PON ports will be represented as a switch and all PON tenants will be represented as a port.	HA 330
1.0.1.27	Shall utilize the NE driver model to generate a standard YANG model for the NE	HA 400
1.0.1.28	Generated YANG models will be supported by OpenDayLight and ONOS	HA 410
1.0.1.29	Shall provide interface to publish event and usage data to an Apache Kafka subscriber	HA 500
1.0.1.30	Data publisher shall be encrypted over SSL	HA 510
1.0.1.31	Abstract the interface to the vendor provided device drivers to interface to the specific hardware element.	HA 600
1.0.1.32	Communication shall occur over Secure RCP channel	HA 610
1.0.1.33	Please provide information on the security aspects of the hardware communication.	HA 620
1.0.1.34	Modular NE driver should be provided that will support an OpenSource Abstraction Layer	HA 630
1.0.1.35	Models shall be provided mapping the NE Driver to the abstraction framework	HA 640
1.0.1.36	All flow related capabilities of the NE driver shall be mapped to OpenFlows	HA 650
1.0.1.37	All configuration capabilities of the NE driver shall be mapped to NETCONF	HA 660
1.0.1.38	All performance and logging shall be mapped to NETCONF	HA 670
1.0.1.39	Shall provide a IEEE 1904 driver abstraction and model	HA 680
1.0.1.40	All NE configuration and management capabilities shall be exposed via NETCONF interface	A 1130
1.0.1.41	All Inventory items shall be provided by NETCONF interface	A 1140
1.0.1.42	Configuration Parameters - YANG Model for VF parameters shall be provided	V 1350
1.0.1.43	Configuration Agent - NETCONF over SSH shall be provided	V 1360
1.0.1.44	Configuration/Notification Protocol - NETCONF/YANG RFC list should be supported, other options based on HTTP and/or NETCONF CLI with common scripting options (e.g. Python, Chef, etc.) are being evaluated.	V 1370
1.0.1.45	Network Model to define the network configuration for the VF, including integration with physical network functions (PNFs).	V 1480
1.0.1.46	The vendor shall allow changes to VF configuration without the need to bounce the VM container.	V 1640
1.0.1.47	AT&T will have different operating models where the virtualized components reside resident inside the OLT, local in the site and/or at a remote location.	M 20
1.0.1.48	Network Device should automatically establish connectivity to a vOLT hardware abstraction layer.	M 30
1.0.1.49	YANG models for exposed services on Network Element	A 79

Requirement ID	Requirement Description 1.0.1 – NAL General Requirements	RFP Requirement ID
1.0.1.50	UML models of exposed interfaces	A 560
1.0.1.51	YANG models for exposed NETCONF services for access devices	A 570
1.0.1.52	Shall support the abstracted protocols to network element hardware abstraction driver layer	A 30
1.0.1.53	Shall support NETCONF to OMCI abstraction	A 40
1.0.1.54	Shall support interface to Performance Management Extension	A 50
1.0.1.55	Shall support interface to PON Management Extension	A 60
1.0.1.56	All NETCONF commands shall be defined in a standard YANG model. Non-Standard models shall be submitted to the appropriate standards body within 6 months of draft.	A 1020
1.0.1.57	All NE capabilities shall be modeled in YANG	A 1120
1.0.1.58	All of the CLI commands supported by the NE shall be exposed via a structured representation defined with one or more vendor provided YANG Models (e.g., YANG models covering Interfaces, VLANs, Routing Protocols, Security ACLs).	E 980
1.0.1.59	The YANG models should be published and installable on a 3rd. Party (external) SDN Controller for interaction with the NE.	E 990
1.0.1.60	The YANG models shall preferably re-use standard models, where available, such as from OpenDayLight.	E 1000
1.0.1.61	Vendor shall provide all such YANG models currently supported by the NE, and identify mapping to CLI.	E 1010
1.0.1.62	Vendor shall include a roadmap stating when additional YANG Models will be available.	E 1020
1.0.1.63	NE shall support configuration of all features and functions proposed for AT&T's implementation via the NETCONF [IETF RFC 6241] protocol.	E 1220
1.0.1.64	All NETCONF Protocol Operations and sub-operations specified in the standard must be supported including configuration and roll-back on error.	E 1230

User Story 1.1: Standard Extensions for NAL

As a Service provider, we want to develop extensions to a standard abstraction layer so that we can facilitate the adaptation of the OLT Control plane protocols (initially OpenFlow). This abstraction layer will also facilitate the adaptation of the OLT management plane protocols (initially NETCONF/YANG).

Assumptions

- Key functions are identified in order to make standard – all Silicon should perform the same/Like Functions
- Common requirements are met that are provided in EPIC_COMMON.docx

Acceptance Criteria

- Functions to be properly documented tested & validated.
- Meet the defined test plan developed. To be delivered 4Q2016
- OpenFlow Table Management Interface
- OpenFlow pipeline Management Interface
- 10G XGS Data model for management and control for OLT system, PON and ONTs
- Support for various hardware device drivers (See 1.1.3.1)

Requirements

1.1.1 - OLT Functions

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.1	NAL shall support the setup of IEEE 802.3ad ling aggregation, with LACP signal on all OLT uplink interfaces.	L 110
1.1.1.2	NAL shall support the configuration of OLT Link Aggregation Group (LAG) hashing options: a) Source/destination MAC address; b) VLAN tag; c) Source/destination IP address	L 120
1.1.1.3	NAL shall support the ability to configure up to eight links in a LAG groups.	L 140
1.1.1.4	Shall support the configuration of broadcast suppression based on pps (packets per second), on a VLAN basis.	L 210
1.1.1.5	NAL shall support control flow handling between ONOS and the OLT as defined by 802.3x PAUSE mechanism for all Ethernet interfaces.	L 290
1.1.1.6	NAL shall support control flow handling between ONOS and the OLT.	L 300
1.1.1.7	Shall support the configuration of the OLT for priority based flow control per IEEE 802.3Qbb.	L 310
1.1.1.8	NAL shall have the ability to support the LAG configuration per OLT	L 340
1.1.1.9	NAL Shall support the configuration of 5 VLAN tags with deep packet inspection for at least 2 tags.	L 350
1.1.1.10	NAL shall support the Pushing, Popping and swapping of VLAN tags.	L 360
1.1.1.11	The NAL shall support a unique PON ID value of each channel termination shall have a manufacturer-set default value composed of the vendor code agreed between the vendor and the operator, and a unique vendor-specific number.	L 380
1.1.1.12	Shall have the ability to configure the PON for different window/fiber distance for ONT operations. MIN/MAX ranges shall be configurable in the system.	L 610
1.1.1.13	Shall allow configurable downstream and upstream PON FEC (On or OFF) on a per ONT basis.	L 620
1.1.1.14	Shall support TWDM PON channels on any combination of OLT ports belonging to one OLT.	L 710

Information herein is a “Contribution” submitted under ONOS Agreement between AT&T Services, Inc. and Open Networking Laboratory dated 1/1/14.

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.15	Shall allow creation of administrative TWDM domains within the same single OLT.	L 720
1.1.1.16	Should allow creation of administrative TWDM domains across multiple OLT.	L 730
1.1.1.17	Shall be able to identify the administrative TWDM domain it belongs to within a TWDM PON system on the PON interface.	L 740
1.1.1.18	Shall be able to identify the administrative TWDM domain it belongs to within a TWDM PON system on the PON interface.	L 740
1.1.1.19	Shall comply with Inter-OLT-port management protocol as detailed in G.989.3.	L 750
1.1.1.20	Channel map configuration, status sharing, ONU tuning, and protection switching functionalities within a single TWDM administrative domain shall be enabled through OLT port configuration.	L 760
1.1.1.21	Shall support both ONU activation and rogue ONU mitigation within the entire TWDM system.	L 770
1.1.1.22	Shall support capabilities as defined in ITU-T G.989	L 780
1.1.1.23	Shall support configurable protection within a single TDWM channel as part of the same TWDM PON.	L 790
1.1.1.24	Shall support ONT activation states, messages, and procedures as specified in G.989.3.	L 810
1.1.1.25	Shall support ONT tuning states, messages, and procedures as specified in G.989.3.	L 820
1.1.1.26	Shall support the configuration of closed-loop automatic Tx tuning control for the subtending ONTs.	L 830
1.1.1.27	Shall support the configuration of MAC layer Access Control Lists (ACLs) to permit or deny based on source, or on destination, or on both source and destination MAC addresses.	L 840
1.1.1.28	Shall support the configuration of MAC filtering in ingress and egress directions.	L 850
1.1.1.29	Shall support the configuration of the filtering function described in IEEE802.1D.	L 860
1.1.1.30	Shall support the configuration of MAC layer ACLs to permit or deny based on source MAC address.	L 870
1.1.1.31	Shall support the configuration of MAC layer ACLs to permit or deny based on destination MAC address.	L 880
1.1.1.32	Shall support the configuration of static entries into the filtering database, where both allowed and disallowed addresses for each possible outbound port may be configured for each bridge port, including each bridge port associated with each Ethernet Interface.	L 890
1.1.1.33	Shall be able to support configuration of Ethernet frame MTU in 4 byte increments.	L 910
1.1.1.34	Shall support the configuration of MTU sizes of at least up to 9k bytes on all the Ethernet interfaces.	L 920
1.1.1.35	Shall support the configuration of Ethernet Bridging per IEEE802.1D-2004	L 930
1.1.1.36	Shall support VLAN tagging, per IEEE 802.1Q-2011.	L 940
1.1.1.37	Shall support VLAN Stacking, per IEEE 802.1ad Provider Bridges.	L 950
1.1.1.38	Customer VLAN tag(s) received within the customer's PON XGEM Port-ID in the OLT shall be retained (honored), removed, changed, or Q-in-Q encapsulated (nested) based on provisioning options available to the service provider.	L 960
1.1.1.39	Customer VLAN tag(s) received within the subscriber's port shall be retained (honored), removed, changed, or Q-in-Q encapsulated (nested) based on provisioning options available to AT&T.	L 1000
Requirement	Requirement Description	RFP

ID	1.2.1 – OLT Functions	Requirement ID
1.1.1.40	VLAN tags on marked traffic received on the ingress of the OLT's network-facing Ethernet port/s shall be retained (honored), discarded, or overwritten based on provisioning options available to AT&T.	L 980, L 1020
1.1.1.41	NAL shall be able to support the configuration of the attachment of an S-Tag or C-Tag to untagged frames received on the user ports in the upstream direction.	L 1030
1.1.1.42	Shall support use of one or more S-Tag per TWDM channel on a PON port.	L 1050
1.1.1.43	NAL shall be able to support the configuration of the attachment of an S-Tag to C-Tag frames received on the user ports in the upstream direction.	L 1060
1.1.1.44	Shall allow the configuration of an S-Tag and/or C-Tag to OLT-initiated frames (e.g., management) in the upstream and downstream directions.	L 1070
1.1.1.45	NAL support the ability to configure the removal or addition of the VLAN Tag Identification for the OLT.	L 1080
1.1.1.46	Shall support the configuration of the Ethertype field for 802.1ad tagging, i.e., S-Tags, shall support at least the standardized value 0x88a8.	L 1090
1.1.1.47	Shall allow per-port configuration of the 'acceptable frame types' to be one of the following values: 'VLAN tagged', 'untagged or priority-tagged' and 'admit all' (i.e., accepting VLAN-tagged, untagged and priority-tagged frames). Frames not matching the configured 'acceptable frame types' shall be discarded.	L 1100
1.1.1.48	Shall support configuring a port to be VLAN transparent (i.e., enabled for TLS).	L 1110
1.1.1.49	For each VLAN-transparent port, shall allow AT&T to indicate a list of C-VIDs, denoted as the port's VLAN membership list, that are allocated for non-TLS traffic. Any frame received on a user-facing TLS enabled port untagged or not matching with a C-VID from the port's VLAN membership list shall be forwarded as TLS traffic.	L 1120
1.1.1.50	For each VLAN transparent port, shall allow AT&T to configure a set of S-VIDs and C-VIDS, denoted as the port's TLS membership list, that are allocated for TLS traffic. Any double-tagged frame received on a user-facing TLS-enabled port and matching the list will be forwarded into the corresponding VLAN.	L 1130
1.1.1.51	Shall support the configuration for sharing of TLS S-VIDs among multiple-user ports.	L 1140
1.1.1.52	For each VLAN transparent port, shall allow AT&T to configure one of the following priority marking options that will be used for marking the S-Tag encapsulating tagged TLS traffic: a. Ingress to egress Priority mapping b. Copy ingress (802.1Q tag) priority to S-Tag.	L 1150
1.1.1.53	Shall support the configuration to remove S-Tag from any frame destined to a given VLAN transparent user port carrying a TLS S-VID.	L 1160
1.1.1.54	For each VLAN transparent port, shall allow AT&T to configure a VLAN translation table, consisting of an entry for each VLAN in the port's VLAN membership list. This table can be used for: a. Indicating an S-VID to replace the U-interface C-VID, if the C-Tag needs to be replaced with an S-Tag. b. Indicating both a C-VID and an S-VID, if the U-interface C-VID has to be overwritten and the frame needs also S-Tag attachment.	L 1170
1.1.1.55	In the downstream direction the OLT shall perform the reverse translation and required tag modification described in the preceding requirement in order to reproduce the U-interface C-VIDs. The priority marking of the received downstream frame C-Tag, however, is not modified.	L 1180

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.56	For each C-VID in a given port VLAN membership list, shall allow AT&T to indicate whether to accept (i.e., forward 'as is') the received VLAN priority markings or rewrite the priority using an ingress-to-egress priority mapping. In the latter case, the priority mapping shall be configurable (per C-VID in the port's VLAN membership list).	L 1190
1.1.1.57	For each port configured as 'untagged or priority-tagged' or 'admit all', shall allow AT&T to configure whether it requires insertion of an S-Tag, or both C-Tag and S-Tag to received untagged and priority-tagged frames.	L 1200
1.1.1.58	For each port configured as 'untagged or priority-tagged' or 'admit all', shall allow AT&T to configure whether it requires insertion of an S-Tag, or both C-Tag and S-Tag to received untagged and priority-tagged frames.	L 1200
1.1.1.59	For each port configured as 'untagged or priority-tagged' or 'admit all', shall allow AT&T to configure whether it should copy the priority marking of the received upstream priority-tagged frame to the S-tag (and C-tag, if applicable) or whether it should override it using an ingress-to-egress priority mapping.	L 1210
1.1.1.60	For each port configured as 'untagged or priority-tagged' or 'admit all', shall allow the following S-Tag parameters to be configurable per port: a. S-VID, b. S-Tag priority.	L 1220
1.1.1.61	For each port configured as 'untagged or priority-tagged' or 'admit all', shall allow the following C-Tag parameters to be configurable per port (assuming C-Tag attachment is enabled for this port): • C-VID • C-Tag priority.	L 1230
1.1.1.62	Any untagged or priority-tagged frame received on a port configured as 'untagged or priority-tagged' or 'admit all' shall be tagged with the configurable default tagging, unless matching an Ethertype filter associated with this port.	L 1250
1.1.1.63	Any frame destined to a given user port (*i.e.*, in the downstream direction), carrying the port's default tagging, shall be forwarded downstream as an untagged frame.	L 1260
1.1.1.64	Shall be able to assign an Ethertype filter to a given port. At a minimum, the following types shall be supported: • PPPoE (Ethertype =0x8863 and 0x8864) • IPoE (Ethertype=0x0800) • ARP (Ethertype=0x0806) • IPv6 (Ethertype=0x86DD).	L 1270
1.1.1.65	Once a frame is classified, shall be able to set the: • S-VID and C-VID that will be used for tagging the filtered frames. These S-VID and C-VID (if applicable) are denoted a 'filter assigned tagging'. • VLAN priority. In the case of priority-tagged frames, this will be either the received priority or the outcome of ingress-to-egress priority mapping respective to whether the received tags were copied or overwritten.	L 1280
1.1.1.66	Any frame destined to a given user port (*i.e.,* in the downstream direction), carrying a filter-assigned tagging, shall be sent out as an untagged frame.	L 1290
1.1.1.67	For each port configured for receiving VLAN-tagged frames (i.e., acceptable frame type of 'VLAN tagged' or 'admit all'), Shall allow AT&T to indicate a list of C-VIDs, denoted as the port's VLAN membership list that are acceptable for this port. In this case, the OLTs shall discard any VLAN-tagged frame received from a port with non-compliant C-VID.	L 1300

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.68	For each port configured for receiving VLAN-tagged frames, shall allow AT&T to configure a VLAN translation table consisting of an entry for each VLAN in the port's VLAN membership list and VID value(s) to translate it to. This table can be used for: a. Indicating an S-VID to replace the U-interface C-VID, if the C-Tag needs to be replaced with an S-Tag. b. Indicating both a C-VID and an S-VID, if the U-interface C-VID has to be overwritten and the frame needs also S-Tag attachment.	L 1310
1.1.1.69	In the downstream direction, shall support the configuration of the OLT to perform the reverse translation and required tag modification described in the preceding requirement, in order to reproduce the U-interface C-VIDs. The priority marking of the received downstream frame C-Tag, however, is not modified.	L 1320
1.1.1.70	Shall support the configuration of the VLAN membership list to indicate whether to accept (i.e., forward 'as is') the received VLAN priority markings or rewrite the priority using an ingress to egress priority mapping. Shall support the configuration of the priority mapping per C-VID in the port's VLAN membership list.	L 1330
1.1.1.71	Shall support the following VLAN allocation paradigms: • Assigning the same S-VID to a group of ports. This paradigm is denoted N:1 VLAN to indicate many-to-one mapping between ports and VLAN. Example criteria for grouping are same originating VP, same service, and same 'destination' service provider. • Assigning a unique VLAN identification to a port using either a unique S-VID or a unique (S-VID, C-VID) pair. The uniqueness of the S-VID shall be maintained in the aggregation network. This paradigm is denoted 1:1 VLAN to indicate a one-to-one mapping between port and VLAN.	L 1340
1.1.1.72	Shall support the configuration of Jumbo Ethernet frames.	L 1350
1.1.1.73	Shall support the configuration of N:1 VLAN forwarding, i.e., determining the destination port according to the MAC address and the S-VID.	L 1360
1.1.1.74	Shall be able to configure the prevention of forwarding traffic between user ports (user isolation) per S-VID.	L 1370
1.1.1.75	Shall support the configuration of 1:1 VLAN forwarding.	L 1380
1.1.1.76	Shall support the configuration of downstream mapping between S-VLAN and port.	L 1390
1.1.1.77	Shall support the configuration of downstream mapping between S-VLAN and C-VLAN pair and port. (Add MPLS)	L 1400
1.1.1.78	Shall be able to disable MAC address learning for 1:1 VLANs.	L 1410
1.1.1.79	Shall support the configuration of forwarding traffic rules based on subscriber VLAN ids and MAC Addresses	L 1420
1.1.1.80	Shall be capable of forwarding all traffic received from a subscriber physical port to a configured destination port or MAC address.	L 1430
1.1.1.81	Shall be able to configure the OLT to block subscriber traffic to/from duplicate MAC addresses across different VLANs on a given OLT. If a duplicate MAC address is detected, increment a counter and log the details of the address and associated port information	L 1440
1.1.1.82	Shall support the bridging of MAC packets among XGEM Port-IDs by default.	L 1470
1.1.1.83	Shall support LLDP, per IEEE 802.1AB-2009.	L 1480
1.1.1.84	Shall support ability to detect loop at the Ethernet port.	L 1490

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.85	Shall support the ability to map each individual XGEM Port-ID from a PON interface to a specified VLAN on the 10GigE/40GigE/100GigE interface(s), and vice versa. Either a single XGEM Port-ID or multiple XGEM Port-IDs should be able to be mapped to a single VLAN through provisioning.	L 1530
1.1.1.86	Shall support per-VLAN per-service queuing/scheduling on the egress of uplinks.	L 1540
1.1.1.87	Shall support mapping of XGEM Port-IDs on the PON side to eight (8) priority levels on the Ethernet side.	L 1550
1.1.1.88	Shall support the configuration and management of device priority queues.	L 1560
1.1.1.89	Shall support at least 8 traffic classes for Ethernet frames and shall support configurable mapping to these classes from the 8 possible values of the Ethernet priority field.	L 1570
1.1.1.90	Shall support the configuration of ingress policing by classified flow.	L 1580
1.1.1.91	Shall support the configuration of a minimum of 8 policers per subscriber physical port.	L 1590
1.1.1.92	Shall support the configuration of IEEE 802.1Q User priority bits (formerly 802.1P bits).	L 1600
1.1.1.93	Shall support the ability to configure any combination of CoS p-bit values to any of the egress queues.	L 1610
1.1.1.94	Shall support provisioning options for priority marking bits for traffic received on the ingress of the PON system's Ethernet port. (e.g. retained (honored), discarded, or overwritten)	L 1620
1.1.1.95	Shall support provisioning options for priority marking bits for traffic received on the ingress of the Subscriber-facing port. (e.g. retained (honored), discarded, or overwritten)	L 1630
1.1.1.96	Shall support the configuration of work-conserving scheduling schemes, where each queue in the WRR/WRED queue scheduler has the ability to take full available bandwidth in the absence of traffic in the other queues.	L 1690
1.1.1.97	Shall support the ability to map each individual subscriber Port to a specified VLAN on any network 10GigE/40GigE/100GigE interface, and vice versa. Either a single subscriber port or multiple subscriber ports should be able to be mapped to a single VLAN through provisioning.	L 1700
1.1.1.98	Shall support configuration of per-VLAN per-service queues/schedules on the egress of uplinks.	L 1710
1.1.1.99	Shall support the configuration of eight (8) Ethernet P-bit marks per 802.1Q	L 1720
1.1.1.100	Shall support the configuration of a minimum of eight (8) queues on the upstream and downstream port(s) in support of priority levels (one per traffic class).	L 1730
1.1.1.101	Shall support configurable mapping to these classes from the eight (8) possible values of the Ethernet priority field.	L 1740
1.1.1.102	Shall support the configuration of the PON system elements shall support direct indication of drop precedence within all supported traffic classes based on the DEI bit value of the Ethernet header.	L 1750
1.1.1.103	Shall support the configuration of network queue according to strict priority among at least four (4) queues.	L 1760
1.1.1.104	Shall support setting a CIR for VLANs on network-facing ports and should not exhibit blocking among similar traffic classes among different VLANs.	L 1790

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.105	Shall be able to mark or re-mark the Ethernet priority bits based on the following classification criteria: • User port (physical or logical) • Ethertype (i.e., Ethernet Protocol ID) • Received Ethernet priority bits • IP protocol ID (specifically support classification of IGMP).	L 1800
1.1.1.106	Shall support configurations of marking the TOS bits in the IP header of the OLT-initiated traffic based on the following classification criteria: • User port (physical or logical) • Ethertype (i.e., Ethernet Protocol ID) • IP protocol ID (specifically support classification of IGMP) • IP protocol port number.	L 1810
1.1.1.107	Shall allow the configuration and mapping of Ethernet priority/code points into queue priority.	L 1820
1.1.1.108	For Business Ethernet services, Shall support the configuration of the OLT to transparently switch all traffic arriving over the uplink as user data. In particular, the OLT must transparently pass all L2CPs, ARP, and IGMP messages without proxying, snooping, or filtering. This is defined as the transparent cross-connect mode of the OLT per S-VLAN.	L 1830
1.1.1.109	For Business Ethernet services, Shall support the configuration of the OLT to be able to pass the customer VLAN tag, if such a tag exists, untouched when sending traffic downstream. In particular, the S-VLAN ID and the 802.1p field value must be used to determine the queuing behavior downstream.	L 1840
1.1.1.110	MAC address learning should be configurable per customer connection and should be disabled by default for cross-connect mode used for business Ethernet Services.	L 1850
1.1.1.111	Shall support multicast as defined in ITU G.989.	L 1870
1.1.1.112	Shall be capable of selecting, replicating and forwarding a minimum of 64 unique and active IGMP-controlled multicast groups (channels) per subscriber data port. (includes PIP Mosaic and PEG applications)	L 1880
1.1.1.113	Shall support replicating 4096 active, simultaneous and unique IGMP-controlled multicast groups at a minimum, limited only by the total interface bandwidth.	L 1900
1.1.1.114	Shall support matching groups conveyed by IGMP messages to a list of groups (whitelist) corresponding to a multicast VLAN associated with the port.	L 1910
1.1.1.115	Shall support 8192 unique multicast addresses (whitelist) at a minimum.	L 1920
1.1.1.116	Shall be capable of processing 512 IGMP messages per second.	L 1940
1.1.1.117	Shall support IGMP v3 snooping both with and without proxy reporting (RFC3376 and RFC4541).	L 1950
1.1.1.118	Shall support IGMP v3 Source Specific Multicast (SSM) (RFC4604).	L 1960
1.1.1.119	Shall support the identification and processing of user-initiated IGMP messages.	L 1970
1.1.1.120	Shall support the configuration of IGMP message forwarding or dropping when IGMP is disabled per subscriber port and/or VLAN.	L 1980
1.1.1.121	Shall support dropping of all IGMP messages received on a user port and/or VLAN.	L 1990, L 2050
1.1.1.122	Shall support configurable treatment of IGMP messages that do not match the list of groups (whitelist).	L 2000
1.1.1.123	Shall support the capability of disabling multicast CAC on a per-multicast-VLAN basis.	L 2010

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.124	Shall support the capability of disabling multicast CAC mechanism on a per-subscriber-port basis.	L 2020
1.1.1.125	Shall support the configurable capability of either transparently forwarding or dropping subscriber IGMP messages when IGMP is disabled on a port and/or VLAN.	L 2040
1.1.1.126	Shall have the ability to configure the OLT to copy the frame to the IGMP snooping function, forward it as user data or drop it upon receipt of an IGMP v3 report carrying information on a mix of 'matching' and 'non-matching' multicast groups.	L 2070
1.1.1.127	Shall support the configuration to stop user ports injecting multicast traffic to the aggregation network. This behavior shall be configurable per port and/or VLAN.	L 2080
1.1.1.128	Shall be able to configure a rate limit on IGMP messages on each user port to prevent IGMP flooding attacks.	L 2100
1.1.1.129	Shall be able to configure an IGMP v3 (as per RFC 3376) transparent snooping and proxy function. This feature shall be configurable on a per VLAN basis. Note: V3 includes support of earlier versions of IGMP. Specifically, this function is responsible for configuring multicast filters such that packet replication is restricted to those user ports that requested receipt.	L 2110
1.1.1.130	Shall support the configuration of marking user-imitated upstream IGMP traffic with Ethernet priority bits.	L 2170
1.1.1.131	Shall support the configuration of user initiated IGMP messages forwarding to a given multicast VLAN to which that user is attached.	L 2180
1.1.1.132	Shall support configuring which user ports are members of a multicast VLAN.	L 2190
1.1.1.133	Shall support the configuration of IP multicast groups or ranges of multicast groups per multicast VLAN based on: • Source address matching • Group address matching.	L 2200
1.1.1.134	Shall be able to configure per-user-port the maximum number of simultaneous multicast groups allowed.	L 2210
1.1.1.135	Shall support the enabling and disabling handling of various IGMP versions. IGMP v1 shall be dropped by default.	L 2220
1.1.1.136	Shall support the configuration of IGMP v2 and IGMP v3 transparent snooping function. This feature shall be configurable on a per-VLAN basis.	L 2230
1.1.1.137	Shall support the configuration of IGMP v2 and IGMP v3 snooping with proxy reporting. This feature shall be configurable on a per-VLAN basis.	L 2240
1.1.1.138	Shall support the configuration of IGMP v2 and IGMP v3 proxy function. This feature shall be configurable on a per-VLAN basis.	L 2250
1.1.1.139	Shall allow selection between IGMP transparent snooping and proxy reporting on a per-multicast VLAN basis.	L 2260
1.1.1.140	The proxy-reporting and proxy functions shall support marking with Ethernet priority bits the IGMP traffic that the OLT initiates. This feature shall be configurable by AT&T.	L 2270
1.1.1.141	Support for configuring IGMP snooping with proxy reporting function and shall support IGMP proxy query functions.	L 2280
1.1.1.142	Shall support the provisioning of the IGMP rate (IGMP messages per second) allowed per TDWM channel, per PON port as well as per PON card.	L 2290
1.1.1.143	Shall support the threshold alarms for the latency of Ethernet (either multicast or unicast) packets through the OLT (shall not exceed 15ms.)	L 2300

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.144	Shall support the threshold alarms for the delay variation or jitter of Ethernet packets (either multicast or unicast) through the OLT (shall not exceed 10ms.)	L 2310
1.1.1.145	Shall support the threshold alarms for the OLT time to complete all IGMP- join operations (in snooping or proxy mode) (shall not exceed 25 ms)	L 2320
1.1.1.146	Shall support the threshold alarms for the OLT to complete all IGMP-leave operations (in snooping or proxy mode) (shall not exceed 15 ms)	L 2330
1.1.1.147	Shall support the configuration of a Maintenance-association Intermediate Point (MIP) function on a per-user-port and per-VLAN basis.	L 2340
1.1.1.148	Shall support configuration of a Linktrace Reply (LTR) function for each MIP.	L 2350
1.1.1.149	Shall support configuration of Loop Back Reply (LBR) function for each MIP	L 2360, L 2430
1.1.1.150	Shall support configuration of filtering CFM Ethernet OAM messages arriving on a user port. Specifically, the OLT should support discarding LTMs arriving on a user port.	L 2370
1.1.1.151	Shall support configuration of rate limiting of CFM Ethernet OAM messages arriving on a user port. The rate shall be configurable per port.	L 2380
1.1.1.152	In the Carrier maintenance level, shall provide support for an “inward-facing” (“Up”) MEP on every user port (i.e., access loop termination) and per-VLAN basis. In a basic implementation, this could be achieved via the “Bridge Brain/Master Port” model; in which case it shall be noted that this MEP will not be used to test the actual data path through the switch fabric of the OLT.	L 2390
1.1.1.153	Shall support the configuration of MIP as follows: • Per 1:1 VLAN: a MIP on a per-network port and per C-VLAN basis (the S-VLAN appended at the network port is allocated a MEP at the Intra-Carrier level). • Per N:1 VLAN: a MIP on a per-network port and per S-VLAN basis.	L 2400
1.1.1.154	Shall support the configuration of a Loopback Message (LBM) towards its peer MEP(s) and receiving the associated Loopback Reply (LBR), for the MEP on the user port.	L 2410
1.1.1.155	Shall support the configuration of the OLT for receiving a Loopback Message (LBM) from its peer MEP(s) and initiating the associated Loopback Reply (LBR), for the MEP on the user port.	L 2420
1.1.1.156	Shall support the configuration of the OLT for initiating a Linktrace Message (LTM) towards its peer MEP(s) and receiving the associated LinkTrace Reply (LTR), for the MEP on the user port.	L 2440
1.1.1.157	Shall support the configuration of the OLT for receiving a Linktrace Message (LTM) from its peer MEP(s) and initiating the associated LinkTrace Reply (LTR), for the MEP on the user port.	L 2450
1.1.1.158	Shall support the configuration of the OLT for receiving a Linktrace Message (LTM) from its peer MEP(s) and initiating the associated LinkTrace Reply (LTR), for the MIP on the network port.	L 2460
1.1.1.159	Shall support populating the table with <MEP name, MAC address> associations for its peer MEP(s).	L 2470
1.1.1.160	For business customers and/or premium customers requiring proactive monitoring, shall support configuring the generation of Continuity Check Messages (CCMs) for the MEP on the user port.	L 2480
1.1.1.161	Shall support turning off sending of CCMs (i.e., CCM source function disabled and sink function enabled) for the MEP on the user port, while keeping the associated MEP active.	L 2490

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.162	Shall support the configuration for receiving AIS messages on the MEP on the user port (at a so-called inferior Maintenance Level) and send out an AIS message at the next-superior Maintenance Level (i.e., towards the RG).	L 2500
1.1.1.163	Shall support the configuration of outward-facing Maintenance-association End Point (MEP) on a per-network-port and per S-VLAN basis.	L 2510
1.1.1.164	Shall support the configuration of initiating a Loopback Message (LBM) towards its peer MEP(s) and receiving the associated Loopback Reply (LBR), for the MEP(s) on the network port.	L 2520
1.1.1.165	Shall support the configuration of receiving a Loopback Message (LBM) from its peer MEP(s) and initiating the associated Loopback Reply (LBR) for the MEP(s) on the network port.	L 2530
1.1.1.166	Shall support the configuration of initiating a Linktrace Message (LTM) function towards its peer MEP(s) and receiving the associated LinkTrace Reply (LTR) for the MEP(s) on the network port.	L 2540
1.1.1.167	Shall support the configuration of receiving a Linktrace Message (LTM) and initiating the associated Linktrace Reply (LTR) towards its peer MEP(s) for the MEP(s) on the network port.	L 2550
1.1.1.168	Shall support generating Continuity Check Messages (CCMs) for the MEP(s) on the network port.	L 2570
1.1.1.169	Shall support turning off sending of CCMs for the MEP(s) on the network port, while keeping the associated MEP active.	L 2580
1.1.1.170	Shall support receiving AIS messages on the MEP(s) on the network port (at a so-called inferior Maintenance Level) and send out an AIS message at the next-superior Maintenance Level.	L 2590
1.1.1.171	Shall support a Maintenance-association End Point (MEP) on a per-VLAN basis.	L 2600
1.1.1.172	Shall support a default ME level value of 1 for the Access Link level.	L 2610
1.1.1.173	Shall support the configuration of a Loopback Message (LBM) function that can generate a Multicast LBM towards the RG. This requirement allows the OLT to discover the MAC address of the RG and also tests the connectivity to that MEP.	L 2620
1.1.1.174	Shall support sending a loopback request, when receiving a Loopback Reply (LBR), the OLT shall return the RG’s MAC address.	L 2630
1.1.1.175	Shall support the configuration of a Loopback Reply (LBR) function towards its peer MEP(s), in response to a unicast or multicast LBM.	L 2640
1.1.1.176	Shall support a means (NETCONF) for the SDN to configure and monitor IEEE 802.1ag CFM OAM and to allow reporting of status and AIS alarms to the SDN.	L 2660
1.1.1.177	Shall have ability to propagate Ethernet link failure between ONT and CPE/NID towards OLTs connected to WAN port(s) of the OLT.	L 2690
1.1.1.178	Shall support OLT Link OAM (per IEEE 802.3-2005, Clause 57 and 802.3ah Link OAM) on Gigabit Ethernet and 10 Gigabit Ethernet interfaces. Full standards support is required, including Active/Passive modes, Discovery, Critical Events (Dying Gasp, RFI), and Link Monitoring. Any exception shall be explicitly noted by the vendor.	L 2700
1.1.1.179	Shall forward upstream and downstream DHCP packets to be handled by the SDN controller in order to discover mapping of IP address to MAC address and populate its ARP table accordingly.	L 3060
1.1.1.180	Shall ensure that downstream broadcast ARP requests are not sent on access ports that do not have the associated requested IP address.	L 3070

Information herein is a “Contribution” submitted under ONOS Agreement between AT&T Services, Inc. and Open Networking Laboratory dated 1/1/14.

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.181	Shall trap events from the OLT when an IP address spoof attempt occurs	L 3080
1.1.1.182	Shall support the vendor specific/defined attribute of DHCP Option 82 in which the vendor and model of the OLT are each uniquely identified in separate attribute fields of Option 82.	L 3090
1.1.1.183	The value of the Agent Circuit ID shall be explicitly configurable, per individual access loop and logical port. When not explicitly configured, it shall be automatically generated using the default or flexible syntax.	L 3100
1.1.1.184	The value of Access-Node-Identifier shall be configurable per Network element, using an element management interface. The Access-Node-Identifier may be derived automatically from an already defined object ID (e.g., IP address of management interface).	L 3110
1.1.1.185	It shall be possible to override the default syntax of circuit ids, and let the operators configure a more flexible syntax for the Agent Circuit ID, with flexibility in the choice of elements used in the automated generation of circuit-IDs. Such syntax is unique per Network element. The flexible syntax shall allow the concatenation of 2 types of elements: • Strings of ASCII characters configured by the network operator. This will typically include characters used as separators between variable fields (usually “#” “.” “,” “;” “/” or space). • Variable fields whose content is automatically generated by the OLT. Fields should include information which doesn’t vary over time for a given access loop.	L 3120
1.1.1.186	Shall support IPv4 and IPv6 simultaneously without performance degradation.	L 3150
1.1.1.187	Shall support requirements defined in RFC 2460, "Internet Protocol, Version 6 (IPv6) Specification.	L 3180
1.1.1.188	Shall support requirements defined in RFC 2463, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification."	L 3190
1.1.1.189	Shall support requirements defined in RFC 2464, "Transmission of IPv6 Packets over Ethernet Networks."	L 3200
1.1.1.190	Shall support requirements defined in RFC 2474, "Definition of the Differentiated Services Field (DS Field) in the IPv6 Headers."	L 3210
1.1.1.191	Shall support configuring the ICMPv6 as defined in RFC4443.	L 3220
1.1.1.192	Shall support configuring IPv6 based data services.	L 3230
1.1.1.193	Shall support configuring the DHCP snooping function, if used on the OLT, shall support DHCP v6.	L 3240
1.1.1.194	Shall support configuring the ARP proxy function on the OLT, if present, shall support IPv6.	L 3250
1.1.1.195	All data service functionality supported as part of IPv4 implementation shall be supported for IPv6 based data service.	L 3260
1.1.1.196	Shall support configuring the IPv6 multicast based on RFC 3810 and RFC 4604.	L 3270
1.1.1.197	All the IPTV functionality supported as part of IPv4 implementation must be supported for IPv6 based Multicast.	L 3280
1.1.1.198	If at the ONT discovery stage, the transmission within a quiet window remains unparsable, shall instruct the OLT to use the Disable_Discovery codepoint of the Deactivate-Serial_Number PLOAM message to deactivate the potentially offending ONT(s).	L 3290

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.199	Shall support the configuration of the ONT equalization delay and timing thresholds. [Information] If at the ONT ranging stage, the OLT is unable to adjust the ONT's equalization delay so that the ONT's transmission timing falls within the margin of ±8 bits (with respect to the upstream line rate), the OLT shall deactivate the ONT using its discovered Serial Number.	L 3300
1.1.1.200	Shall support the configuration of the ONT transmission drift for each individual ONT, and implement in-service equalization delay adjustment using the drift timing thresholds. [Information] OLT shall monitor the upstream transmission drift for each individual ONT, and implement in-service equalization delay adjustment using the drift timing thresholds equivalent of ±8 bits and ±16 bits with respect to the upstream line rate. The drift correction shall not cause any customer service impact.	L 3310
1.1.1.201	Shall support the configuration of the OLT for rogue interference detection in the upstream transmission, including alarm thresholds and whether detection is enabled or disabled. Detection of interference shall be logged.	L 3320, L3330, L3350
1.1.1.202	For each monitored condition, upon detection of a rogue interference event, shall be able to set a separate alarm to the SDN.	L 3360
1.1.1.203	For each monitored condition, it shall be possible to support alarming of detected rogue interference events.	L 3370
1.1.1.204	Upon detection of a rogue interference event, the OLT shall implement the techniques for isolating and identifying the ONU-ID and the Serial Number of the offending ONT.	L 3380
1.1.1.205	Shall implement the extended Rogue mitigation capability, using the Disable_Discovery code point of the Disable_Serial_Number PLOAM message.	L 3390
1.1.1.206	Upon detection of a rogue interference event, shall support increasing of the interburst guard times as a means of the offending ONT isolation and identification.	L 3400
1.1.1.207	Upon detection of a rogue interference event, shall support dynamic rearrangement of the upstream transmissions in time as a means of the offending ONT isolation and identification.	L 3410
1.1.1.208	Upon detection of a rogue interference event, shall support temporary relocation of the known ONTs to different TWDM channels as a means of the offending ONT isolation and identification.	L 3420
1.1.1.209	Upon detection of a rogue interference event or a missed allocation, shall use the inter-OLT-port management channel to coordinate rogue ONT isolation and identification with the other OLTs of the PON system.	L 3430
1.1.1.210	Shall support parsing of an unexpected well-formed upstream transmission as a means of the offending ONT isolation and identification.	L 3440
1.1.1.211	Shall respond to and cooperate with other OLTs of the PON system that use the inter-OLT-port management channel for the rogue ONT isolation, identification, and mitigation purposes.	L 3450
1.1.1.212	Upon detection of a rogue interference event, the OLT shall temporarily disable the known ONTs and subsequently re-enabling them as a means of the offending ONT isolation and identification.	L 3460
1.1.1.213	For each rogue ONT isolation and identification technique employed by your implementation, it shall be possible to activate/deactivate the technique via the SDN.	L 3480

Requirement ID	Requirement Description 1.2.1 – OLT Functions	RFP Requirement ID
1.1.1.214	For each rogue ONT isolation and identification technique employed by your implementation, it shall be possible to specify the order (after, before, concurrent with) of its application via the SDN.	L 3490
1.1.1.215	Shall implement a set of techniques for mitigating the rogue ONT behavior in the upstream transmission. Use G.Sup49 as a reference.	L 3500
1.1.1.216	When able to identify the serial number of the offending ONT, shall support disabling of the offending ONT by sending a Disable_Serial_Number downstream PLOAM message.	L 3520
1.1.1.217	When informed of the serial number of the offending ONT via an inter-OLT-port management channel, it shall support disabling of the offending ONT by sending a Disable_Serial_Number downstream PLOAM message.	L 3530
1.1.1.218	Please describe the rogue ONT mitigation techniques employed by your implementation that specifically address the rogue interference events associated with the multiwavelength nature of the TWDM PON system. Discuss how each technique will be tested and experimentally verified.	L 3540
1.1.1.219	Upon detection of a rogue interference event affecting a given TWDM channel, shall support evacuating the working ONTs to alternative TWDM channels within the TWDM PON system.	L 3550
1.1.1.220	Shall respond to SDN-directing loop-back activation and deactivation commands at the physical layer.	L 3700
1.1.1.221	Should support the pre-provisioning of ports, services and subscribers on that hardware prior to the device being installed.	L 3730
1.1.1.222	If pre-provisioning ports, shall send an error message to the SDN if a port type other than the pre-provisioned type has been installed in the target port.	L 3740
1.1.1.223	During initial ONT turn up, after the ONT is powered up and ONT serial number sent to the OLT, the ONT shall range; come up on its startup code; and send information on its current software version (stored internally). Shall determine if the ONT software needs to be upgraded. If an upgrade is needed, shall initiate the ONT upgrade process.	L 3940
1.1.1.224	It shall be possible to retrieve the type, model and version of ONTs on the OLT.	L 3980
1.1.1.225	After the target ONT software transfer is complete and successful, there shall be positive indication provided regarding the code version present on the ONT. An “Auto ONT Upgrade Successfully Complete” trap shall be generated.	L 4020
1.1.1.226	If there is an error or failure associated with the target ONT software download process, the download process shall be attempted again. A configurable number of retry attempts shall be initiated (default:3)	L 4030
1.1.1.227	If the upgrade process fails after the 3rd attempt, a trap shall be provided with any known reason for the failure.	L 4040
1.1.1.228	Shall support hitless automatic and manual (normal and forced) switching operations between redundant units.	L 4110

1.1.2 - ONT Functions

Requirement ID	Requirement Description 1.2.2 – ONT Functions	RFP Requirement ID
1.1.2.1	Shall be capable of supporting the AES security mechanism on the ONT defined in G.989.3.	N 70
1.1.2.2	Shall provide all provisioned services to the customer within 30 seconds when power is returned to a previously provisioned ONT.	N 100
1.1.2.3	Shall provide all services to the customer within 10 seconds when power is returned to a previously provisioned ONT.	N 110
1.1.2.4	Shall support Watchful sleep power management mode per ITU-T G.989.3/G.9807.1.	N 150
1.1.2.5	Upon detection by the ONT watchdog of a transmitter parameter violation, if the detected condition is severe (that is, may be causing immediate disruption to the operation of the PON system), shall notify the ONT to immediately and completely turn the laser OFF.	N 310
1.1.2.6	Upon detection by the ONT watchdog of a transmitter parameter violation, if the detected condition is intermittent or otherwise limited in its impact, the ONT shall perform the following action sequence: (1) set an OMCI alarm; (2) set the embedded Dying Gasp indication; (3) cease upstream data transmission, except PLOAM and OMCI channels; (4) upon 3ms turn the laser OFF completely.	N 320
1.1.2.7	Upon detection by the ONT watchdog of a transmitter parameter violation that requires the laser to be turned OFF, shall capture and store an urgent status snapshot record.	N 330
1.1.2.8	Shall implement the extended Rogue mitigation capability, recognizing the Disable_Discovery code point of the Disable_Serial_Number PLOAM message.	N 340
1.1.2.9	Shall support configuration of local switching between ports on multi data port ONTs. The local switching between data ports shall be disabled by default.	N 530
1.1.2.10	Shall allow for the provisioning of several tiers of data rates [Information] Provisioning starting at 64 Kbps, and continuing up to 10000 Mbps for each 10/100/1000/2.5G/5G/10G BaseT interface with the understanding that 802.3bz has not been adopted.	N 540
1.1.2.11	Shall support the configuration of the ONT and various predefined tiers data rates. [Informational] Starting at 64 Kbps, and continuing up to 10000 Mbps on 10 Gbps copper and optical interfaces.	N 560
1.1.2.12	Shall allow for the remote activation and deactivation of the ONT data services on a per-interface basis. Implementation shall be via the OMCI managed entities.	N 570
1.1.2.13	Each data interface of the ONT should support a minimum of 128 MAC addresses in the filtering tables that are associated with that interface, where up to 1/4 of these entries may be statically configured in the “permanent” database.	N 650
1.1.2.14	Shall support the configuration of static entries into the filtering database, where both allowed and disallowed addresses for each possible outbound port may be configured for each bridge port, including each XGEM Port-ID bridge port.	N 660

Requirement ID	Requirement Description 1.2.2 – ONT Functions	RFP Requirement ID
1.1.2.15	Shall support a configuration option that allows only the operator to configure the static filtered addresses for each port of the bridge (data interface and GEM Port-IDs). This configuration should be consistent with the Bridge Management features described in IEEE 802.1D.	N 670
1.1.2.16	Shall support the port rate configuration (or auto-negotiate) of the ONT Ethernet UNI port	N 690
1.1.2.17	Shall support the alarming of transmitted optical power is to high alarm when reaching the preconfigured threshold (default > +7dBm)	N 1340
1.1.2.18	Shall support the alarming of transmitted optical power is to low alarm when reaching the preconfigured threshold (default < +2dBm)	N 1350
1.1.2.19	Shall support the alarming of received optical power is to high alarm when reaching the preconfigured threshold (default > -7dBm)	N 1360
1.1.2.20	Shall support the alarming of received optical power is to low alarm when reaching the preconfigured threshold (default < -28dBm)	N 1370
1.1.2.21	Shall support the configuration of ONT Tx for FEC ON and FEC OFF modes, making the selection between the two modes according to the burst profile specified.	N 1390
1.1.2.22	Shall invoke the FEC-transparent mode under OMCI control while processing FEC-enabled traffic stream.	N 1430
1.1.2.23	Shall support connectivity to the OLT support link OAM (per IEEE 802.3-2005, Clause 57). Full standards support is required, which includes Active/Passive modes, Discovery, Critical Events (Dying Gasp, RFI), and Link Monitoring.	N 2530
1.1.2.24	Shall support configuration of the CFM messages for MD level on the OLT. The CFM messages for other MD level shall not be send to processor for any processing and should be filtered in the fast path.	N 2550
1.1.2.25	Shall support the configuration and management of the device capabilities for IETF RFC 5357, A Two-Way Active Measurement Protocol (TWAMP).	N 2690
1.1.2.26	All IEEE 802.1ag, ITU-T Y.1731, ITU-T Y.1564, IETF RFC 2544 and TWAMP traffic must be processed at the hardware level so it will minimize the impact to normal CPU processing of other traffic.	N 2730
1.1.2.27	Shall support configuration of H.248 Gateway Control Protocol.	N 3720
1.1.2.28	TDM Voice will be supported via AT&T's existing G6 Voice Gateways.	N 3730

1.1.3 - NAL Integration Support

Requirement ID	Requirement Description 1.2.3 – NAL Integration Support	RFP Requirement ID
1.1.3.1	Integration with various implementations and (OLT to ONT) combinations of the following hardware: - 1 Broadcom Maple B0 based Pizzaboxes - 1 Broadcom Maple B0 based Hardened Clamshell - 1 MicroOLT - 1 FPGA Based Pizzabox - 1 FPGA Based Clamshell - Up to 8 ONT/NTE Hardware specific selection will be provided by 4Q2016	A 21
1.1.3.2	Shall support testing of up to 128 Split Ratio	A 22
1.1.3.3	Shall collaborate with the Driver developers in the integration into the hardware abstraction layer	A 71
1.1.3.4	Shall provide any development and integration required to integrate the device driver into the abstraction layer. This includes the Broadcom and TiBit hardware drivers.	A 72
1.1.3.5	Shall support Baseline and Extended OMCI message format.	I 100
1.1.3.6	Shall support OMCI-based ONT software image download using extended OMCI message format (1955 bytes).	I 110
1.1.3.7	Shall must support ONU Remote Debug standard ME.	I 120

User Story 1.2: Enhanced Extensions for NAL

As a service provider to operationalize the access network it is required to have management tooling for the support of the physical network devices. To avoid multiple vendor specific implementations of element managements systems (EMS) it is desired to abstract and standardize common system functionality through the NAL. A standard set of tooling and interface is required to integrate into a common management platform. Initially it is desired to standardize on the software upgrade and PON management capabilities of the access platform.

Assumptions

- If possible, we will utilize existing Indigo and OVS software solutions to be run in a standard Network Abstraction Layer to help facilitate standardization
- Common requirements are met that are provided in EPIC_COMMON.docx
- Design should not be restricted to OLT and ONT capabilities in order to implement other access technologies.

Acceptance Criteria

- Ability to utilize OpenFlow for the OLT Control plane
- Ability to utilize NETCONF for the OLT management plane
- Ability to perform software upgrades on the OLT
- Ability to perform software upgrades on the ONT
- Ability to collect and performance measures off of the OLT and ONT.
- Ability to provide performance data through a Kafka data provider interface
- Abstraction of the OMCI capabilities through a NETCONF interface
- Ability to retrieve and provide inventory information of the managed devices.
- Ability to manage and configure the OLT and ONT devices
- Meet the defined test plan developed. To be delivered 4Q2016

Requirements

1.2.1 – Software Upgrades

Requirement ID	Requirement Description 1.1.1 – Software Downloads	RFP Requirement ID
1.2.1.1	The Abstraction Layer shall perform software downloads in a non-service affecting manner. (Hitless Upgrade support) (Note: These downloads can be performed during any time of day.)	M 3001
1.2.1.2	Abstraction Layer shall support pushing software updates to network devices	M 3002
1.2.1.3	NAL shall perform a backup of the software and configuration prior to performing the software update	M 3003
1.2.1.4	Abstraction Layer shall capture, log and notify the state of the software upgrade process	M 3004
1.2.1.5	NAL shall support software downloads to the OLT	
1.2.1.6	NAL shall support software downloads to the ONT	
1.2.1.7	NAL shall support scheduling of the downloads	
1.2.1.8	NAL shall support on demand, parallel and serial software downloads to the managed devices. Deployment method shall be selectable through the service API.	
1.2.1.9	Ability perform software upgrade over OMCI.	HA 740
1.2.1.10	Ability to perform automatic device upgrades in the event the newly download version does not match the running image.	HA 780
1.2.1.11	Upgrades shall be initiated through NETCONF request to the abstraction layer	HA 770
1.2.1.12	Shall maintain image and hash of operating image	HA 750
1.2.1.13	Shall compare hash and date of new images to the currently deployed image in order to determine if an upgrade is required	HA 760

Requirement ID	Requirement Description 1.1.1 – Software Downloads	RFP Requirement ID
1.2.1.14	Shall have ability to download device images through SFTP and HTTPS	HA 800
1.2.1.15	Shall support configuration of automatic upgrades (enable/disable) and ability to specify an execution time	

1.2.2 - PON Management Extension

Requirement ID	Requirement Description 1.1.2 – PON Management Extensions	RFP Requirement ID
1.2.2.1	All ONT OMCI service shall be mapped to NAL's protocol abstraction layer (Initially this will be focused as NETCONF protocol interface).	HA 700
1.2.2.2	All OMCI service mappings to NETCONF shall be defined in a YANG model.	HA 710
1.2.2.3	Ability to schedule a time or time window to perform upgrades.	HA 790
1.2.2.4	Ability to block/unblock an ONT from communicating with other systems.	HA 820
1.2.2.5	Ability to configure a blocking time window of 10 Minutes to ONT	HA 830
1.2.2.6	Shall provide reset capability to the ONT	HA 840
1.2.2.7	Shall provide Inband Link establishment	HA 850
1.2.2.8	Compliance with ITU G.983.2 and G.984.4 Standards	HA 861
1.2.2.9	Shall maintain OMCI channel through keep-alives	HA 863
1.2.2.10	Shall provide automated Link status	HA 864
1.2.2.11	Shall detect gaps in the receipt of loggable events and create a warning log in the abstraction layer	HA 867
1.2.2.12	Shall prevent log storms by detecting and consolidating identical events and create the appropriate warning or error log events in the abstraction layer	HA 868
1.2.2.13	Compliance with ITU G.988 and 9807.1 Standards	HA 869
1.2.2.14	Shall provide ability to Admin the PON port state	HA 1000
1.2.2.15	Shall provide Line level monitoring of both TX and RX	HA 1010
1.2.2.16	Shall support ONT Detection and Activation	HA 1020
1.2.2.17	Shall provide Software Management capabilities for the PON and exposed through NETCONF interface	HA 1030
1.2.2.18	Shall support ONT alarm handling to NETCONF interface	HA 1040
1.2.2.19	Shall detect Rogue ONT modules and issue alarms through NETCONF interface.	HA 1050
1.2.2.20	Shall support the enabling and disabling of FEC for the PON link	HA 1060
1.2.2.21	Provides Wavelength management and optimization for tunable optics.	HA 1070
1.2.2.22	Allows for interoperable with BBF.247 certified ONUs.	HA 1090
1.2.2.23	Shall be Interoperable with various OLTs.	HA 1100
1.2.2.24	Shall provide Bridge Port Provisioning	HA 1110
1.2.2.25	Shall provide configuration of Ingress QoS Profile at OLT (GEM Port)	HA 1120
1.2.2.26	Shall provide configuration of Upstream Bandwidth Profile at ONT (Tcont)	HA 1130
1.2.2.27	Shall support PON Monitoring/Alarms, Counters, SFP Management, Housekeeping	HA 1150
1.2.2.28	Support Timing synchronization to the ONT by utilizing the host time.	HA 1160
1.2.2.29	Shall provide configuration of Downstream/Upstream Bandwidth DBA Profile at ONT (Tcont)	HA 1130
1.2.2.30	Shall collect performance measures for each network element such as: packets sent/received, dropped packets, retransmits, FEC, GEMs.	HA 1200
1.2.2.31	Shall provide power measurement information for the Network element including system power and optical power measures	HA 1210
1.2.2.32	Shall support ITU Y.1731 for Ethernet	HA 1220
1.2.2.33	Scheduling shall be exposed through a NETCONF interface	